

Cisco Business Dashboard and Probe Quick Start Guide

First Published: 2020-07-13

Last Modified: 2026-01-21

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.


The Java logo is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. or other countries.

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Cisco Business Dashboard Overview** 1

About Cisco Business Dashboard 1

Device Management Mode 2

Audience 2

Related Documents 2

Terminology 3

CHAPTER 2 **Performing Initial Setup for the Dashboard** 5

Performing Initial Setup for the Dashboard 5

CHAPTER 3 **Performing Initial Setup for the Probe** 9

Performing Initial Setup for the Probe 9

CHAPTER 4 **Performing Initial Setup for Direct Managed Devices** 15

Performing Initial Setup for Direct Managed Devices 15

CHAPTER 5 **Setting Up the Network** 19

Setting Up the Network for Cisco Business Dashboard 19

Setting Up Network Plug and Play 22

Configuring the Network 24

CHAPTER 6 **Frequently Asked Questions** 27

General FAQs 27

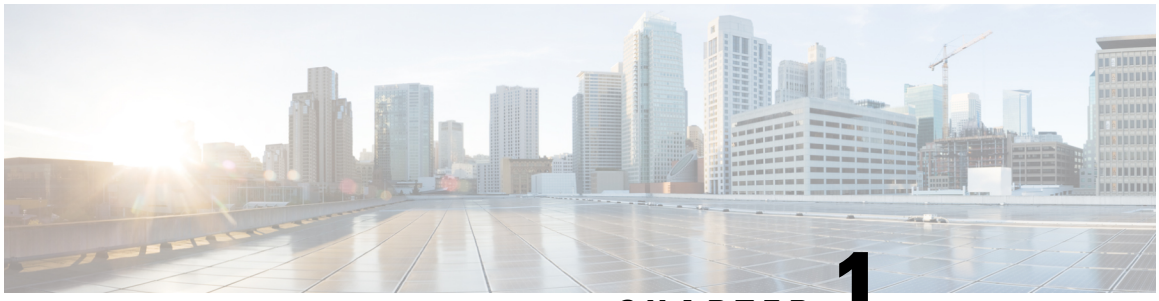
Discovery FAQs 28

Configuration FAQs 29

Security Consideration FAQs 30

Remote Access FAQs 36

Software Update FAQs 36



CHAPTER 1

Cisco Business Dashboard Overview

This chapter contains the following sections:

- About Cisco Business Dashboard , on page 1
- Device Management Mode, on page 2
- Audience, on page 2
- Related Documents, on page 2
- Terminology, on page 3

About Cisco Business Dashboard

Cisco Business Dashboard provides tools that help you monitor and manage the devices in your Cisco Business network. It automatically discovers your network, and allows you to configure and monitor all supported devices such as switches, routers, and wireless access points. It also notifies you about the availability of firmware updates, and about any devices that are no longer under warranty or covered by a support contract.

You can view the application by clicking Request a Demo

Cisco Business Dashboard is a distributed application which is comprised of two separate components or applications as described below:

The Dashboard

Cisco Business Dashboard also referred to as *the Dashboard*, is installed at a convenient location in the network. From the Dashboard user interface, you can get a high-level view of the status of all the sites in your network, or concentrate on a single site or device to see information specific to that site or device.

The Probe

Cisco Business Dashboard Probe also referred to as *the Probe* is installed at each site in the network and associated with the Dashboard. The probe performs network discovery and communicates directly with each managed device on behalf of the Dashboard.

Note Certain network devices support being directly associated with the Dashboard and managed without a probe being present. When network devices are being managed directly in this way, all management functions are available for the device, but the network discovery process may not be as comprehensive as when a probe is present.

Device Management Mode

Direct Managed

Certain devices can support direct association with the Dashboard and managed without a probe being present in the network.

In a direct managed network, you will need to connect the first device to the Cisco Business Dashboard manually. Then, this device reports information such as CDP, LLDP, and mDNS (aka Bonjour) to Dashboard. This information is used to identify additional devices in the network, Dashboard then connects these devices to itself automatically hence those devices become manageable, and the process repeats until all devices have been discovered. Depending on the size of your network, this process may take tens of minutes. You may optionally have the dashboard explicitly search the IP address ranges to discover network devices, which can be in other VLANs or subnets.

Direct managed network is recommended if all your devices support direct management.

Probe Managed

Probe is installed at each site in the network and associated with the Dashboard. The Probe performs network discovery and communicates directly with each managed device on behalf of the Dashboard.

A software Probe is a probe running in a virtual machine or on a Linux host. A software Probe can generally manage up to 50 network devices. Certain devices include the Probe application embedded in the device firmware. An embedded Probe can manage up to 15 network devices.

In one network you should only enable one Probe.

Audience

This guide is primarily intended for network administrators who are responsible for Cisco Business Dashboard software installation and management.

Related Documents

The documentation for Cisco Business Dashboard is comprised of a number of separate guides. These include:

- **Quick Start Guide (this document)**—This guide provides details on performing the initial setup for Cisco Business Dashboard using the most commonly selected options.
- **Installation Guides**

  The following table lists all the installation guides for the Dashboard software that can be deployed on different platforms. Refer the path provided in the location column for details:

Supported Platforms	Location
Microsoft Azure	Cisco Business Dashboard & Probe Installation Guide for Microsoft Azure
Amazon Web Services	Cisco Business Dashboard & Probe Installation Guide for Amazon Web Services (AWS)

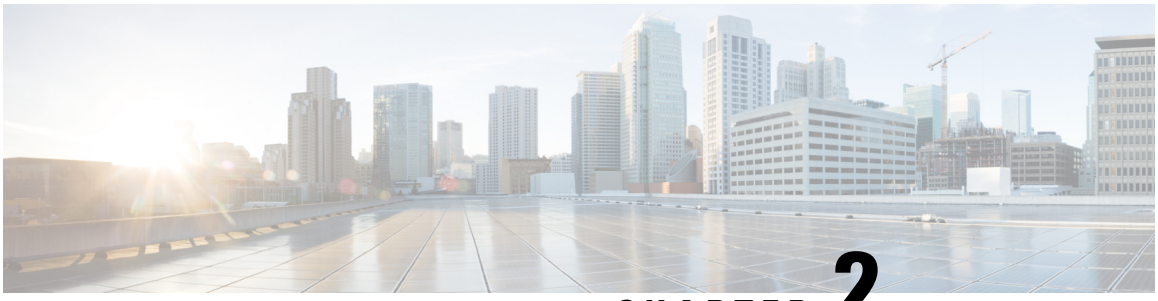
Supported Platforms	Location
Oracle VirtualBox	Cisco Business Dashboard & Probe Installation Guide for Oracle VirtualBox
Microsoft Hyper-V	Cisco Business Dashboard Installation Guide for Microsoft Hyper-V
VMWare vSphere, Workstation and Fusion	Cisco Business Dashboard &Probe Installation Guide for VMWare
Ubuntu Linux (Dashboard and Probe) and Raspbian Linux (Probe only)	Cisco Business Dashboard &Probe Installation Guide for Linux

- **Administration Guide**—This is a reference guide that provides details about all the features and options provided by the software and how they may be configured and used. Refer to Cisco Business Dashboard Administration Guide.
- **Device Support List**—This list provides details of the devices supported byCisco Business Dashboard and the features available for each device type. For a list of all the devices supported by Cisco Business Dashboard, refer to Cisco Business Dashboard - Device Support List.

Terminology

Term	Description
Hyper-V	A virtualization platform provided by Microsoft Corporation.
Open Virtualization Format (OVF)	A TAR archive containing one or more virtual machines in OVF format. It is a platform-independent method of packaging and distributing Virtual Machines (VMs).
Open Virtual Appliance or Application (OVA) file	Package that contains the following files used to describe a virtual machine and saved in a single archive using **.TAR** packaging: • Descriptor file (.OVF) • Manifest (.MF) and certificate files (optional)
Raspberry Pi	A very low cost, single board computer developed by the Raspberry Pi Foundation. For more information, see *https://www.raspberrypi.org/*.
Raspberry Pi OS	Formally known as Raspbian, the Raspberry Pi OS is a Debian-based linux distribution optimized for the Raspberry Pi. For more information, see *https://www.raspberrypi.org/software/*.
VirtualBox	A virtualization platform provided by Oracle Corporation.
Virtual Hard Disk (VHD)	Virtual hard disk is a disk image file format for storing the complete contents of a hard drive.

Term	Description
Virtual Machine (VM)	A virtual computing environment in which a guest operating system and associated application software can run. Multiple VMs can operate on the same host system concurrently.
• VMWare ESXi • VMWare Fusion • vSphere Server • VMWare Workstation	A virtualization platform provided by VMWare Inc.
vSphere Client	User interface that enables users to connect remotely to vCenter Server or ESXi from any Windows PC. You can use the primary interface for vSphere Client to create, manage, and monitor VMs, their resources, and the hosts. It also provides console access to VMs.
Hypervisor	Also known as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs). A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing.
Amazon Web Services (AWS)	An on-demand cloud computing platform.
Micosoft Azure Active Directory	A cloud-based identity and access management service that provides single sign-on and multi-factor authentication to help protect users from 99.9 percent of cybersecurity attacks.



CHAPTER 2

Performing Initial Setup for the Dashboard

• Performing Initial Setup for the Dashboard, on page 5

Performing Initial Setup for the Dashboard

There are a few configuration tasks that should be performed to ensure that the Dashboard meets your requirements.

Configuring Basic System Settings

To configure basic system settings such as IP addressing and time settings for the Dashboard, follow the steps below:

1. Connect to the console of the Dashboard using the appropriate tools for your hypervisor if using a virtual machine, or by connecting to your AWS or Azure instance using SSH
2. If using a virtual machine, log in using the default username and password set to: `cisco`. For an AWS instance, use the key pair you specified when the instance was created, and the username: `cisco`. For an Azure instance, use the administrator username and password or key you specified when creating the instance.

   You will be required to change the password for the cisco account immediately after logging in. The new password should be a complex, non-dictionary word using a mixture of character types.
3. Enter the command `sudo config_vm` to perform the initial configuration. When prompted, enter the password for the cisco account. The `config_vm` utility will prompt you with a series of steps to change the platform settings.
4. First you will be prompted to change the hostname for the Dashboard. The hostname is used to identify the Dashboard on the network. Choose a meaningful name here, or you can skip this step to keep the default hostname.
5. Next you will be prompted to change the web server ports. If these ports are changed from the default values, it may also be necessary to change firewall settings in your network, or security group settings in AWS or Azure.
6. Next you will be prompted to configure the network interface. The options here are static and dhcp (the default). If you select static, you will be prompted for IP address information, default gateway, and DNS server addresses. The network interface will be reset if you make changes here.

Performing Initial Setup for the Dashboard

Note This step is not available with Cisco Business Dashboard for AWS or Azure. To modify the network configuration, use the EC2 console in AWS for an AWS instance. Use the Azure Portal for an Azure instance.

7. Next, you will be prompted to configure the time settings for the Dashboard. You can opt to configure one or more NTP servers for time synchronization (recommended), and you will be asked to select the timezone.

Note If the hypervisor in use is VirtualBox and the VirtualBox Guest Additions are installed in the VM, the NTP service - timesyncd - will not operate.

8. Finally, you will be asked if you wish to change the bootloader password. The bootloader username and password can be used on the console at system startup to change the system boot process or recover lost operating system passwords. The default bootloader credentials are username: **root** and password: **cisco**.

You can change these settings at any time by re-running the script, or through the web interface at **System**>**Platform Settings**.

Launching the Dashboard User Interface

1. Launch a web browser such as **Google Chrome** or **Microsoft Edge**.
2. In the **Address** field, enter the IP address or hostname of the Dashboard and press **Enter**
3. Enter the default user name: `cisco` and password: `cisco`. If you are using Cisco Business Dashboard for AWS, the default password is the instance ID. You can view the instance ID in the AWS EC2 console.
4. Click **Login**. You will be prompted to change the username and password for the cisco account. Ensure that the new password is at least 8 characters in length contains at least 3 different character classes.
5. Click **Next**. You will be presented with information about how Cisco Business Dashboard uses your data and what information is shared with Cisco. Make any changes appropriate for your organization's requirements before proceeding.
6. Click **Next**. At this point you are given the option to run the System Setup Wizard which walks you though the key configuration elements that should be considered when installing a new dashboard. You may choose to continue with the wizard by clicking **Next**, or you may click **Finish** to exit to the dashboard UI.

If you choose to proceed with the System Setup Wizard, it will guide you through each of the following areas:

- Platform Settings, including network setup, webserver and security configuration.
- Email forwarding setup for notifications and alerts.
- Creating additional organizations to help manage complex networks or to deliver managed services.
- Create additional users who can manage the dashboard.
- Choose whether to enable or disable Local Probe.

Note As of Cisco Business Dashboard version 2.11.1, the license setup process has been removed. All management capabilities are now provided at no extra cost, independent of the number of devices under management. If you're running a version earlier than 2.11.1, you must still complete the license setup step. This requirement usually applies to systems managing more than 25 network devices.

For more information on any of the configuration covered by the wizard, consult the corresponding section of the Cisco Business Dashboard Administration Guide.

Disabling the Embedded Probe on the VM Image

Note This does not apply to Cisco Business Dashboard for AWS or Azure.

The virtual machine image for the Dashboard includes the Probe software for managing devices on the network local to the Dashboard. If you do not wish to manage the local network, you can disable the embedded Probe using the following steps:

1. Navigate to **System**>**Local Probe**.
2. Click the toggle switch to disable the embedded Probe.
3. Click **Save**.

Create Networks (Optional)

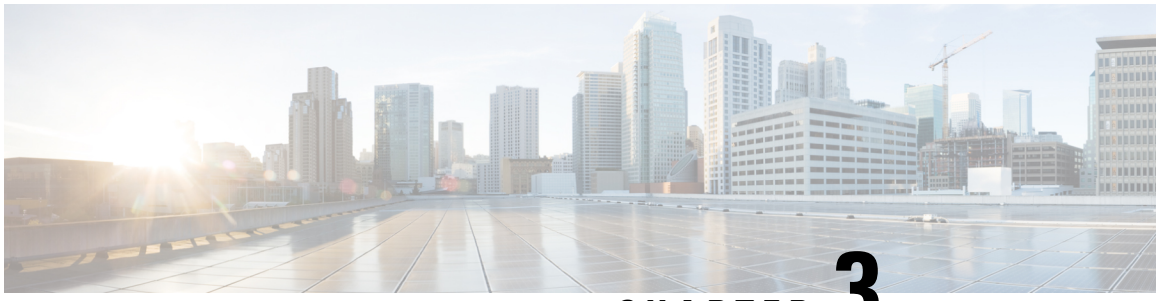
You can pre-define network records in the Dashboard for Probes that you will associate later. Typically, each network represents a separate site, but you can have multiple networks in the same location. To create a new network, follow the steps below:

1. Navigate to **Network**.
2. Click **Add Network** in the **Map View** or **+**(plus) icon in the **List View**.
3. Specific a **Name, Organization** and **Default Device Group** for the network.
4. Optional) Enter the **Management VLAN.** By default, the Dashboard may display any discovered IP address for devices with multiple IP addresses. If you specify a Management VLAN, the IP address of the VLAN interface matching the configured Management VLAN will be shown in the Inventory and Topology views. The Management VLAN setting only determines which IP address is displayed; the Dashboard may still use any discovered, reachable IP address to access the device. Leave this field blank if your device does not have multiple IP addresses.
5. Enter the **Address** of the network into the appropriate fields. If you enter a partial address, a list of potential matches will be displayed, and you can select the location from the list. Alternatively, you can click on the location in the map.
6. Choose the **Network Type.** Select Probe Managed to manage the network using a software or embedded probe, or choose Direct Managed if you want each device to connect and be managed directly by Cisco Business Dashboard. If you choose Direct Managed, You can also enable an option for the Dashboard to automatically enable the CBD agent on any newly discovered devices in the network, allowing them to

connect to Cisco Business Dashboard automatically. Note: A device must connect to Dashboard in order to be managed.

7. Click **Save**.
8. Repeat steps 1 to 5 for each network you wish to create.

   After creating a network, you can click the **Onboard Devices** button on the What's Next page. Once clicked, the Onboarding tab of the network detail page automatically opens, providing a step-by-step wizard that guides you through connecting a Probe or devices to the network.



CHAPTER 3

Performing Initial Setup for the Probe

This chapter contains the following sections:

- Performing Initial Setup for the Probe, on page 9

Performing Initial Setup for the Probe

There are a few configuration tasks that should be performed to ensure that the Probe meets your requirements.

Locating the IP Address of the Probe

To find the IP address being used by the probe, use one of the following methods:

1. The default IP address configuration for the Probe is performed using DHCP. Make sure your DHCP server is running and can be reached. If no DHCP server is available, the IP address will default to 192.168.1.10.
2. The Probe is Bonjour-enabled and automatically advertises itself using the Bonjour protocol. If you have a Bonjour-enabled browser, you can find the Probe on your local network without knowing its IP address.
3. If you are using the virtual machine image, you can retrieve the IP address of the Probe from the virtual machine console. Use your Hypervisor's management tools to connect to the console of the virtual machine and log on with the default username: `cisco` and password: `cisco`. You will be required to change the password immediately after logging in. The new password should be a complex, non-dictionary word using a mixture of character types. A banner will then be displayed showing the current IP address.

   If you have installed the Probe on your own Ubuntu or Raspbian Linux installation, you can use the operating system tools to discover the IP address. For example, you can enter the command `ifconfig` at a shell prompt and see a list of interfaces and their addresses displayed.



Note The credentials set here are used to log on to the probe whenever it is not actively connected to a dashboard. When connected to a dashboard, the probe must be accessed using the same credentials used to log on to the dashboard.

4. Locate the IP address assigned by your DHCP server by accessing your router or DHCP server. See your DHCP server instructions for more information.

Setting Up a Software Probe

A software probe is a probe running in a virtual machine or on a Linux host when there is no Dashboard running on the same VM or host.

To set up a software probe, follow the steps below:

1. Launch a web browser, such as **Google Chrome** or **Microsoft Edge**.
2. In the **Address** field, enter the DHCP-assigned IP address and click **Enter**.
3. Enter the default user name: `cisco` and password: `cisco`. Click **Login**.
4. You will be prompted to change the username and password for the cisco account. Ensure that the new password is at least 8 characters in length using at least 3 different character classes. Click **Save**.
5. Specify the address or hostname of a Dashboard to connect to and click **Next**.
6. Your browser will be redirected to the Dashboard login screen. Login using administrator credentials for the Dashboard.
7. Choose to either create a new network or to select an existing network from the drop-down provided. If you choose to create a new network, then specify a name and location for the network in the boxes provided.

   You can enter the address of the network into the appropriate fields. If you enter a partial address, a list of potential matches will be displayed, and you can select the location from the list. Alternatively, you can click on the location in the map.
8. Click **Finish** to be redirected back to the probe GUI.

Setting up an Embedded Probe on a Small Business Switch

The process for connecting an embedded probe to the dashboard requires explicit configuration on both the Dashboard and Probe prior to connecting. This process can be automated using a zero-touch deployment method such as Network Plug and Play. You can also perform the setup following a step-by-step wizard available in Cisco Business Dashboard: after creating a network (type is Probe Managed) in the Dashboard, click the Onboard Devices button on the What's Next page. This opens the Onboarding tab of the network detail page, where a connection wizard will guide you through the configuration process. Supported devices include:

- Cisco Catalyst 1200/1300 Series Switch
- Cisco Business 250/350 Series Switch
- Cisco 250/350/550 Series Switch

The connection wizard provides specific instructions for each device type. Select your device, then follow the steps for either the device GUI or CLI, as appropriate.

General steps include:

- Verify that the device system time is correct.
- If your device uses a static IP address, ensure the default gateway setting of device is set correctly.
- If the Dashboard server address is specified as a domain name, verify the DNS server setting of device is correct.

If using device CLI

- Check and copy the device Product ID (PID) and Serial Number (SN) to create a new device record in the Dashboard.
- The Dashboard will generate CLI commands to configure the device. Copy and run these commands in the device CLI console.

If using device GUI:

- Specify the address or domain name of the Dashboard and select the connection setup method as "Online with Web Browser".
- Click the Apply button.
- Your browser will be redirected to the Dashboard login screen. Log in using your administrator credentials.
- Choose Associate Network and select the current network from the drop-down provided, click Next.
- Click Finish to be redirected back to the device GUI.

After completing the setup, remember to save the running configuration to the startup configuration to ensure that your changes persist across device reboots. See the device documentation for more details on the location and use of the CBD agent configuration page.



Note The steps below describe how to manually set up a device using the "Offline with Access Key" method. This method is not recommended except for cases where your device is running older firmware or belongs to a legacy device series that does not support the "Online with Web Browser" option. Whenever possible, you should use "**Online with Web Browser**" when connecting your device to Cisco Business Dashboard. This method will automatically download and configure the access key and install the CBD certificate, ensuring the most secure and streamlined setup.

To manually set up an embedded probe, follow the steps below:

1. Create a new network record for the embedded probe using the steps described in Performing Initial Setup for the Dashboard, on page 5.
2. On the Dashboard UI, go to the Inventory and click the plus (+) icon to create a new device record. Fill in the form with appropriate details for the device that will host the probe, making certain to specify the correct product ID and serial number. This will allow the dashboard to associate the probe with the correct network.
3. On the Dashboard UI, go to the **My Profile** page by clicking on your username at the bottom of the navigation panel. Use this page to create a new **Access Key** using the **Generate Access Key** button. You can also use an existing access key if you prefer.



Note The access key used for associating an embedded probe with the dashboard does not need to be a long lived key. This key only needs to be valid at the time the initial association takes place. Once the probe and dashboard are associated, the connection is authenticated using limited access, short-lived credentials that are unique to the network and regenerated periodically.

4. Obtain the root CA certificate from your CBD. On the **Dashboard UI**, go to **System** > **Certificate** and copy the root certificate to your clipboard. Then, on the **device UI**, go to the CA certificate settings page

- typically found under Security > Certificate Settings > CA Certificate Settings on small business switches. Add the certificate by entering a name (no spaces) and pasting the certificate content into the provided field.

5. Using the **device UI,** navigate to the Dashboard configuration page - typically found under Administration > Cisco Business Dashboard Settings on small business switches. Select the connection setup method as "Offline with Access Key". At the minimum, you will need to supply configuration for the dashboard address and port, and access key ID and secret. If the device is running an older version of the CBD agent, you will also need to specify the organization and network names.
6. Submit the changes. The device will connect to the dashboard and be associated with the network created in step 1.

   See the device documentation for more details on the location and use of the CBD agent configuration page.

Verifying the Identity of the Dashboard

When establishing a connection to the dashboard, the probe checks to ensure the certificate presented by the dashboard is valid and can be trusted. For the certificate to be acceptable and the connection to proceed, the certificate must meet the following conditions:

- The certificate must be signed by a trusted Certificate Authority (CA), or the certificate itself must be added to the device configuration as a trusted certificate. Refer the device administration guide for details on adding a trusted certificate.
- If the dashboard is configured as an IP address, then either the Common Name field or the Subject-Alt-Name field of the certificate must contain that IP address
- If the dashboard is configured as a hostname, then either the Common Name field or the Subject-Alt-Name field of the certificate must contain that hostname

Configuring Basic System Settings on the VM image using Web User Interface (Optional)

To configure basic system settings such as IP addressing and time settings for the Probe using the web user interface, follow the steps below:

1. Navigate to **Administration** > **Platform Settings**.
2. Specify a hostname for the Probe. The hostname is used to identify the Probe on the network.
3. Optionally, specify static IP parameters in the fields provided. By default, the Probe will automatically determine the IP settings using DHCP.
4. Alternatively, you can set the Probe to use its internal clock for keeping time, or you can specify your preferred NTP servers. By default, the Probe will synchronize its clock with public NTP servers.



Note If the hypervisor in use is VirtualBox and the VirtualBox Guest Additions are installed in the VM, the NTP service - timesyncd - will not operate.

Configuring Basic System Settings on the VM Image through the Command Line (Optional)

As an alternative to configuring basic system settings through the web interface, you can set them using the command line as follows:

1. Connect to the virtual machine console.
2. Log on using the default username and password set to: `cisco`. You will be required to change the password immediately after logging in. The new password should be a complex, non-dictionary word using a mixture of character types.
3. Enter the command `sudo config_vm` to perform the initial configuration. The `config_vm` utility will prompt you with a series of steps to change the platform settings.
4. First you will be prompted to change the hostname for the Probe. The hostname is used to identify the Probe on the network. Choose a meaningful name here, or you can skip this step to keep the default hostname.
5. Next you will be prompted to change the web server ports. If these ports are changed from the default values, it may also be necessary to change firewall settings in your network.
6. Next you will be prompted to configure the network interface. The options here are static and dhcp (the default). If you select static, you will be prompted for IP address information, default gateway, and DNS server addresses. The network interface will be reset if you make changes here.
7. Next you will be prompted to configure the time settings for the Probe. You can opt to configure one or more NTP servers for time synchronization (recommended), and you will be asked to select the timezone.



Note If the hypervisor in use is VirtualBox and the VirtualBox Guest Additions are installed in the VM, the NTP service - timesyncd - will not operate.

8. Finally, you will be asked if you wish to change the bootloader password. The bootloader username and password can be used on the console at system startup to change the system boot process or recover lost operating system passwords. The default bootloader credentials are username: **root** and password: **cisco**.

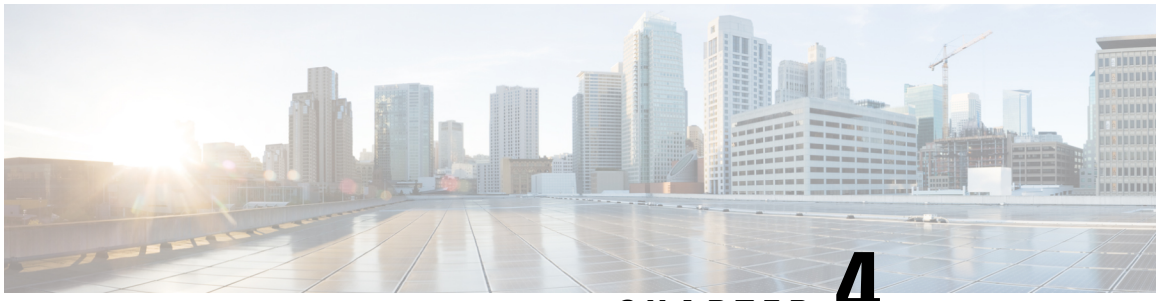
Configuring Basic System Settings when the Probe is Embedded on a Cisco Business Product

If you are using a Probe embedded in a Cisco Business product, then the Probe user interface is accessed through the device administration interface. Consult the device administration guide for more information on associating the Probe with the Dashboard and making changes to system settings.

Configuring Basic System Settings when the Probe is Co-hosted with Cisco Business Dashboard

A Probe that is co-hosted with Cisco Business Dashboard does not have any user interface. The Probe is managed entirely through the Dashboard user interface.

Performing Initial Setup for the Probe



CHAPTER 4

Performing Initial Setup for Direct Managed Devices

This chapter contains the following sections:

- Performing Initial Setup for Direct Managed Devices, on page 15

Performing Initial Setup for Direct Managed Devices

Direct managed devices are network devices that may be associated directly with a Dashboard and managed without a probe being present in the network. Only certain devices support direct management. Refer the Cisco Business Dashboard - Device Support List for a list of devices and software versions that support direct management.

In a directly managed network, **you only need to connect the first supported device to the Cisco Business Dashboard.**This initial device sends information such as CDP, LLDP, and mDNS (Bonjour) to the Dashboard. The Dashboard uses this information to identify additional devices within the network, then automatically connects and manages them. This discovery process repeats itself until all devices are found and managed. After connecting the first device, you can optionally configure the Dashboard to explicitly search specified IP address ranges—using the first device as a proxy—to discover other network devices, including those located in different VLANs or subnets.

The process for connecting a direct managed device to the dashboard requires explicit configuration on both the Dashboard and the device prior to connecting. This process can be automated using a zero-touch deployment method such as Network Plug and Play. You can also perform the setup manually: after creating a network(type is Direct Managed) in Cisco Business Dashboard, click the Onboard Devices button on the What's Next page. This opens the Onboarding tab of the network detail page, where a step-by-step wizard will guide you through the configuration process. Supported devices include:

- Cisco Catalyst 1200/1300 Series Switch
- Cisco Business 250/350 Series Switch
- Cisco Business 220 Series Switch
- Cisco Business 100/200 Series Access Point

The connection wizard provides specific instructions for each device type. Select your device, then follow the steps for either the device GUI or CLI, as appropriate.

General steps include:

Performing Initial Setup for Direct Managed Devices

- Verify that the device system time is correct.
- If your device uses a static IP address, ensure the default gateway setting of the device is set correctly.
- If the Dashboard server address is specified as a domain name, verify if the DNS server setting of the Device is correct.

If using device CLI:

- Check and copy the device Product ID (PID) and Serial Number (SN) to create a new device record on the Dashboard UI.
- The Dashboard will generate CLI commands to configure the device. Copy and run these commands in the device CLI console.

If using device GUI:

- Specify the address or domain name of the Dashboard and select the connection setup method as "Online with Web Browser".
- Click the **Apply** or **Save**.
- Your browser will be redirected to the Dashboard login screen. Log in using your administrator credentials.
- Choose **Associate Network** and select the current network from the drop-down provided, click Next.
- Click **Finish** to be redirected back to the device GUI.

After completing the setup, remember to save the running configuration to the startup configuration to ensure that your changes persist across device reboots. See the device documentation for more details on the location and use of the CBD agent configuration page.

Note The steps below describe how to manually set up a device using the "Offline with Access Key" method. This method is not recommended except for cases where your device is running older firmware or belongs to a legacy device series that does not support the "Online with Web Browser" option. Whenever possible, you should use "**Online with Web Browser**" when connecting your device to Cisco Business Dashboard. This method will automatically download and configure the access key and install the CBD certificate, ensuring the most secure and streamlined setup.

To manually set up a direct managed device, follow the steps below:

1. Optionally create a new network record for the network the device will be installed in using the steps described in Performing Initial Setup for the Dashboard, on page 5.
2. On the **Dashboard** UI, go to the **Inventory** and click the plus (+) icon to create a new device record. Fill in the form with appropriate details for the device that will host the probe, making certain to specify the correct product ID and serial number. This will allow the dashboard to associate the probe with the correct network.
3. On the **Dashboard** UI, go to the **My Profile** page by clicking on your username at the bottom of the navigation panel. Use this page to create a new **Access Key** using the **Generate Access Key** button. You can also use an existing access key if you prefer.



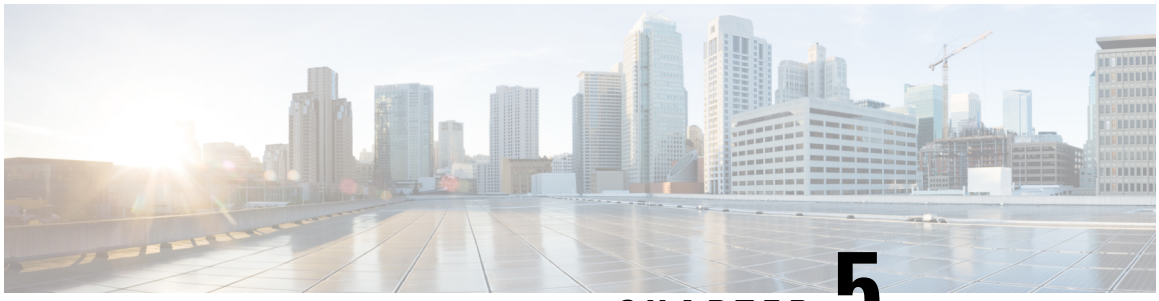
Note The access key used for associating a direct managed device with the dashboard does not need to be a long lived key. This key only needs to be valid at the time the initial association takes place. Once the device and dashboard are associated, the connection is authenticated using limited access, short-lived credentials that are unique to the device and regenerated periodically.

4. Obtain the root CA certificate from your CBD. On the **Dashboard UI**, go to **System** > **Certificate** and copy the root certificate to your clipboard. Then, on the **device UI**, go to the CA certificate settings page - typically found under Security > Certificate Settings > CA Certificate Settings on small business switches. Add the certificate by entering a name (no spaces) and pasting the certificate content into the provided field..
5. Using the **device UI,** navigate to the Dashboard configuration page - typically found under Administration > Cisco Business Dashboard Settings on small business switches or Advanced > CBD Settings on small business APs. Select the connection setup method as "Offline with Access Key". At the minimum, you will need to supply configuration for the dashboard address and port, and access key ID and secret.
6. Submit the changes. The device will connect to the dashboard and be associated with the network created in step 1.

When establishing a connection to the dashboard, the device checks to ensure the certificate presented by the dashboard is valid and can be trusted. For the certificate to be acceptable and the connection to proceed, the certificate must meet the following conditions:

- The certificate must be signed by a trusted Certificate Authority (CA), or the certificate itself must be added to the device configuration as a trusted certificate. Refer the device administration guide for details on adding a trusted certificate.
- If the dashboard is configured as an IP address, then either the **Common Name** field or the **Subject-Alt-Name** field of the certificate must contain that IP address.
- If the dashboard is configured as a hostname, then either the **Common Name** field or the **Subject-Alt-Name** field of the certificate must contain that hostname.

Performing Initial Setup for Direct Managed Devices



CHAPTER 5

Setting Up the Network

This chapter contains the following sections:

- Setting Up the Network for Cisco Business Dashboard, on page 19
- Setting Up Network Plug and Play, on page 22
- Configuring the Network, on page 24

Setting Up the Network for Cisco Business Dashboard

Setting Up Device Credentials

For Cisco Business Dashboard to be able to manage the network devices, you must provide suitable credentials to allow access to each device.

When the Probe discovers a device, it will initially attempt to access the device using the default credentials with the username: `cisco`, password: `cisco` and the SNMP community set to: `public`. However, if the device is not using default credentials, then correct credentials must be supplied as detailed in the following steps:

1. Navigate to **Administration** > **Device Credentials**. The first table on this page lists all the devices that have been discovered that require credentials, while the second table lists all the discovered devices for which working credentials are known.
2. Enter a username and password combination and/or SNMP credentials in the respective fields at the top of the page. If more sets of credentials are required, then click the +(plus) icon. This allows up to three sets of each type of credential to be entered.
3. Click **Apply**. The Probes will test each credential against each device for which a credential is required. Working credentials are saved for each device.

   The Probes will discover each network and generate a topology map and inventory for the network after being provided with the working credentials.

Learn About Your Network

Cisco Business Dashboard provides a high-level view of your network as either a map or a list of networks. To see the high-level view of all networks, perform the following steps:

1. Make sure you have associated your Probes with the Cisco Business Dashboard as described in the previous chapter.

2. Click **Network** in the Dashboard navigation. Click the button to display either the **Map View** or the **List View**.
3. In **Map View**, you may click and drag the map to reposition it, and use the plus and minus buttons to zoom in and out. Each network with a Cisco Business Dashboard Probe installed will be displayed as an icon on the map. Each icon contains a number showing the number of outstanding notifications for that network, and the color of the icon shows the highest severity level outstanding. Click on an icon to see more details about that site. If multiple icons are too close to be easily distinguished, they will be replaced with a cluster marker showing the number of Network icons in that cluster. Click on the cluster marker to zoom in on the sites in that cluster.

   In **List View**, you can click the icon at the top left corner of the table to select the columns to be displayed, and you can click on the column headings to sort the table.
4. Use the Search box to find a specific network or to find the network that contains a particular device. You may enter the name, address or IP address of a network in the Search box, or the name, IP address, MAC address or serial number of a device.
5. When you click on a network, the **Basic Info** panel appears showing you more information about that network. This information includes the network name and address, and a list of outstanding notifications for the network.
6. You may click **More** in the **Basic Info** panel to open up the **Network Detail** a detailed information about that network, including the network topology diagram and floor-plans. It also allows you to modify settings for this network and view all the devices discovered in this network.

You may also use the **Inventory** to see detailed information about all the devices in your network. The **Inventory** page provides a list of all discovered devices in a tabular view. You can filter the list to restrict the devices displayed, and click on individual devices to see more information about that device.

Discover the Network by Scanning IP Addresses (Optional - Direct Managed Networks Only)

For direct managed networks, Cisco Business Dashboard may not always be able to discover network devices in other VLANs or subnets using only the automated discovery processes. When this occurs, it can be beneficial to have the dashboard explicitly search the IP address ranges associated with those VLANs or subnets. To search an IP address range, do the following:

1. Log on to the dashboard administration interface and open the Job Center by clicking on the hourglass icon in the top right corner of the screen.
2. Select the **Schedule Profiles** tab and click the plus (+) icon to create a new schedule profile.
3. Set the Job Type to **Search IPv4 Range for Devices**.
4. Select the appropriate organization and chose the network to search.
5. Set the schedule for the job. Optionally set it to recur periodically if you want to search the network regularly.
6. Specify the credentials to use when discovering devices and specify the IP address ranges to search.
7. Click **Save**.

Based on the schedule, the dashboard will search the specified address ranges for devices with an active web server and attempt to connect to the device using the credentials provided. If the dashboard is successful in

accessing the device, it will be added to the inventory and will be managed in the same way as any other device in the network.

Customizing the Topology Map (Optional)

Once working credentials are provided, the **Probes** or direct managed devices will discover each network and generate a **Topology** map. You may adjust the map as necessary.

1. Navigate to **Network** and select the network of interest. Click **Details** to display the topology.
2. Use **Overlays and Filters** to limit the device types that are displayed in the topology diagram.

Uploading Floor Plans (Optional)

You may upload floor plans for each network and place your network devices in order to document the location of your equipment. The following steps guide you through this process:

1. When viewing the topology diagram for a network, click **Floor Plan**.
2. Enter a name for the building and the floor, and then either drag an image file into the drop zone or click inside the widget to select an image file on your PC. Image formats supported include `.png, .gif, .jpg`
3. Click **Save** to save the changes.
4. To place a device on the floor plan, click **Add Devices** and type the device name or IP address into the search box at the bottom of the screen. Matching devices will be displayed, where grayed out devices have already been placed on a floor plan.
5. Click and drag a device to add it to the floor plan in the correct location.

Customizing the Monitoring Dashboard

You may customize the monitoring dashboard to suit your requirements using the following steps:

1. Select **Dashboard** from the navigation at the left of the screen. The default dashboard will be displayed.
2. To relocate individual widgets within the dashboard, click on the Dashboard Edit icon at the right of the dashboard and select the **Edit Mode** option. Click and hold to drag each widget to the desired location. To resize a widget, click and hold on the edge or corner of the widget to resize.
3. To add a new widget to the dashboard, click the Dashboard Edit icon at the right of the dashboard and select the Edit Mode option. To add a widget, click the + icon beside each widget name. To remove a widget from the dashboard, click **remove widget ✖** icon in the top right corner of the widget when in edit mode.
4. Once the dashboard is laid out correctly, click the Dashboard Edit icon at the right of the dashboard and select **View Mode** to lock the changes in place.
5. To change the behavior of a widget, click **edit widget configuration** icon in the top right of the widget. Use the drop down lists to select the specific device, interface or network the widget should monitor.

Setting Up Network Plug and Play

Cisco Business Dashboard provides a Cisco Network Plug and Play service that allows you to centrally manage firmware and configuration files for selected Cisco devices. For more information about Network Plug and Play, refer to the PnP Solution Guide.

To set up Network Plug and Play, perform the following tasks.

Upload Firmware

1. Navigate to **Provision** > **Network Plug and Play** > **Images**.
2. Click the ✚(plus) icon.
3. Choose an organization and then drag a firmware file from your PC and drop it on the target area of the **Upload File** window. Alternatively, click the target area and select a firmware image to upload.
4. Click **Upload**.

You may designate an image as the default image for one or more device types. To designate an image as a default image, do the following:

1. Select the checkbox for the image in the **Images** table and click **edit**.
2. Enter a comma-separated list of product IDs into the **Default Image for Product IDs** field. Product IDs can contain the wildcard characters '?', representing a single character, and '*', representing a string of characters.
3. Click **save**.

Upload Configurations (Optional)

1. Navigate to **Provision** > **Network Plug and Play** > **Configurations**.
2. Click the ✚(plus) icon.
3. Choose an organization and then drag a configuration file from your PC and drop it on the target area of the **Upload File** window. Alternatively, you can click on the target area and select a configuration file to upload.
4. Click **Upload**.

Instead of uploading configurations, you may make use of the included configuration templates supplied with the Dashboard application. You can click on the name of a configuration file to view the contents if you wish.

Setting up Discovery

In order for network devices to use **Network Plug and Play**, they first need to discover the **Network Plug and Play** server. There are three mechanisms that may be used to provide this information to the devices:

1. **DHCP**: The network device can learn the address of the Network Plug and Play server using DHCP option 43. For more detail on the option format, refer to section, *About Network Plug and Play*, in the Cisco Business Dashboard Administration Guide.

2. **DNS**: If the network device does not learn the server address through DHCP, it will attempt to lookup up a well-known hostname, pnpserver, in the local domain—For example, *pnpserver.example.com*. You may configure your DNS infrastructure to ensure that this name resolves to the address of the Cisco Business Dashboard.
3. **Plug and Play Connect**: Cisco provides a redirection service, **Plug and Play Connect**, that the device will query if it is not able to find the address of the server any other way. To set up the redirection service for your network, please refer to the section *Network Plug and Play* in the Cisco Business Dashboard Administration Guide.

Registering Devices

To register devices in preparation for installation, do the following:

1. Navigate to **Provision > Network Plug and Play** > **Enabled Devices**.
2. Click the ✚ (plus) icon to add devices manually.



Note You may also click the upload icon to add devices in bulk using a csv file. Template csv files may be downloaded from the **Network Plug and Play > Configurations** page by opening the configuration template to be used for the devices and selecting **Download CSV Template** from the **Actions** dropdown.

3. Enter the name, product ID (PID) and serial number of the device to be registered and select an organization, network, device group and device type from the drop-down lists.
4. You may select either or both of a firmware image and configuration file to use for this device. If you choose Default image as the image, the device will use the image designated as the default for that device type at the time the device connects to the server.
5. Click **Save**.

Auto Claiming Devices

A device that connects to the server and is not present in the inventory is considered to be an unclaimed device. Unclaimed devices may be automatically claimed and provisioned by the server by creating an Auto Claim rule for that product ID. To create an Auto-Claim rule, do the following:

1. Navigate to **Provision > Network Plug and Play** > **Auto Claim Devices**.
2. Click the ✚ (plus) icon.
3. Enter the product ID (PID) to automatically claim and select an organization, network, device group and device type from the drop-down lists.
4. You may select either or both of a firmware image and configuration file to use for this product ID. If you choose Default image as the image, auto claimed devices will use the image designated as the default for that device type at the time the device connects to the server.
5. Click **Save**.

Configuring the Network

If you are installing a new network, you may want to take this opportunity to perform the initial configuration of the network. Even in an existing network, you can choose to make configuration changes at this time.

Updating Firmware for devices (Optional)

The Dashboard will notify you if there are firmware updates available for the devices in your network, and an **Update Firmware** icon will be displayed against the device in several areas of the user interface.

To update firmware for a single device, follow the steps below:

1. Click on the device in the **Topology Map** to display the **Basic Info** panel.
2. Open the **Action** panel and click on the **Upgrade firmware to latest** button. The Dashboard will download the necessary firmware from Cisco and apply the update to the device. The device will reboot as part of this process.

   Alternatively, firmware can be upgraded from your PC by clicking the **Upgrade From Local** option and specifying the firmware image to be uploaded.
3. You can view the progress of the upgrade by clicking on the **Task Status** icon in the top right of the user interface.

You can also upgrade individual devices from the **Inventory** view. For details, refer to section, *Viewing Device Inventory*, in the Cisco Business Dashboard Administration Guide.

Updating Firmware for a Network

If you wish to upgrade an entire network to the latest available firmware, follow the steps below:

1. Open the **Network Detail** view for the network you wish to update.
2. Click **Network Actions** at the top of the page and select the **Upgrade Firmware** option. The Dashboard will download the necessary firmware files from Cisco for each device that has an available update, and will apply the update to each device in turn. Each device will reboot as part of this process.
3. You can view the progress of the upgrade by clicking on the **Task Status** icon in the top right of the user interface.

Configuring Device Groups

The Dashboard uses the concept of device groups to allow you to apply configuration to multiple devices at the same time and to ensure that configuration settings match across the network. To allocate devices to a device group, follow the steps below:

1. Navigate to **Administration** > **Device Groups**.
2. Click the ✚ (plus) icon to add a new group.
3. Specify an organization, a name and description for the device group. Click **Save**.
4. To add devices to the device group, click the ✚ (plus) icon in the **Devices** table. Use the search box to find devices to add to the group. Select one or more devices to join the group. Each device can only be a member of one group. If a selected device was previously a member of a different group, it will be removed

from that group. If you wish to remove a device from the group, click the **Delete** icon next to the device, and the device will be moved to the **Default** device group. Device groups can contain a mixture of different device types.

Creating Configuration Profiles

The Dashboard allows you to easily apply common configuration to multiple network devices. You can use the **Network Configuration Wizard** to create configuration profiles for each section of the configuration, or you can create profiles individually. To use the **Network Configuration Wizard**, follow the steps below:

1. Navigate to **Provision > Network Configuration** > **Wizard**.
2. Enter a profile name for the configuration profiles to be created, choose an organization and select one or more device groups to which the configuration will be applied.
3. Click **Next**.
4. Specify the time settings for this group. A **Time Management** profile contains settings for the timezone, daylight savings, and NTP. If you do not wish to create a **Time Management** profile for this group, click **Skip**, otherwise click **Next**.
5. Specify the **DNS settings** for this group. A **DNS Resolvers** profile contains settings for the domain name, and the DNS servers to use. If you do not wish to create a DNS Resolvers profile for this group, click **Skip**, otherwise click **Next**.
6. Specify the user authentication settings for this group. An **Authentication profile** contains settings for the local user database for the devices. If you do not wish to create an **Authentication profile** for this group, click **Skip**, otherwise click **Next**.
7. Specify the Virtual LANs to be created for this group. A VLAN profile contains the details for one or more VLANs. If you do not wish to create a VLAN profile, click **Skip**. To add multiple VLANs, click **Add Another** after completing each VLAN. Click **Next**.
8. Specify the Wireless LANs to be created for this group. A Wireless LAN profile contains the details for one or more SSIDs. If you do not wish to create a Wireless LAN profile, click **Skip**. To add multiple SSIDs, click **Add Another** after completing each SSID. Click **Next**.
9. Review the configuration settings you have made. If you wish to make changes, use **Edit** or **Back** to return to the appropriate screen. Once you are satisfied, click **Finish** to create the profiles and apply to the devices in the selected device groups.
10. You can view the progress of the configuration by clicking on the **Task Status** icon in the top right of the user interface.

Backing Up Device Configurations

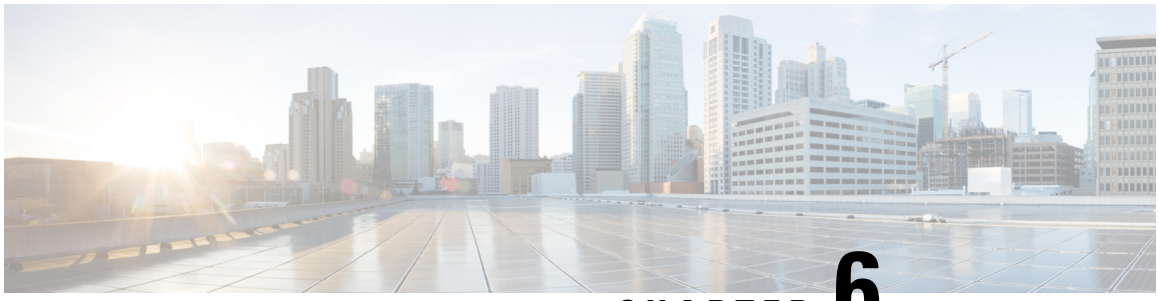
The Dashboard allows you to back up the configurations of your network devices. To back up the configuration for a single device, follow the steps below:

1. Click on the device in the **Topology Map** to display the **Basic Info** panel.
2. Open the **Action** panel and click **Backup Configuration** button. Optionally, you can add a note describing this backup in the window that appears. The **Dashboard** will copy the configuration of the device.
3. You can view the progress of the backup by clicking on the **Task Status** icon in the top right of the user interface.

You can also backup individual devices by clicking **Backup Configuration** in the **Inventory** view.

If you wish to back up the configurations for the entire network, follow the steps below:

1. Open the **Network Detail** view for the network you wish to back up.
2. Click **Actions** button at the top of the page and select the **Backup Configurations** option. Optionally, add a note describing this backup in the window that appears. The Dashboard will copy the configuration of each device.
3. You can view the progress of the backup by clicking on the **Task Status** icon in the top right of the user interface.



CHAPTER 6

Frequently Asked Questions

This chapter answers frequently asked questions about the Cisco Business Dashboard features and issues that may occur. The topics are organized into the following categories:

- General FAQs, on page 27
- Discovery FAQs, on page 28
- Configuration FAQs, on page 29
- Security Consideration FAQs, on page 30
- Remote Access FAQs, on page 36
- Software Update FAQs, on page 36

General FAQs

Q. What languages are supported by the Cisco Business Dashboard?

A. Cisco Business Dashboard is translated into the following languages:

- Chinese
- English
- French
- German
- Japanese
- Portuguese

- Spanish

Q. How can I restart my Cisco Business Dashboard service?
A. Connect to the server console and execute the command "sudo systemctl restart cisco-business-dashboard".

Discovery FAQs

Q. What protocols does Cisco Business Dashboard use to manage my devices?
A. Cisco Business Dashboard uses a variety of protocols to discover and manage the network. Exactly which protocols are using for a particular device will vary between device types.

The protocols used include:

- Multicast DNS and DNS Service Discovery (aka *Bonjour*, see *RFCs 6762 & 6763*)
- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (see *IEEE specification 802.1AB*)
- Simple Network Management Protocol (SNMP)
- RESTCONF (See *https://datatracker.ietf.org/doc/draft-ietf-netconf-restconf/)*
- Proprietary web services APIs

Q. How does Cisco Business Dashboard discover my network?
A. Cisco Business Dashboard uses different discovery processes depending on the network management type:

Direct Managed Network

- You manually connect the first device to the Cisco Business Dashboard.
- This device reports information such as Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), and Multicast DNS (mDNS, aka Bonjour) to the Dashboard.
- The Dashboard uses this information to identify additional devices in the network.
- It then automatically configures these devices to connect to the Dashboard, making them manageable.
- This discovery process repeats until all devices are found.
- Optionally, the Dashboard can explicitly search specified IP address ranges to discover devices in other VLANs or subnets by scanning for devices with active web servers and attempting to connect using provided credentials.

Probe Managed Network

- The Cisco Business Dashboard Probe listens for CDP, LLDP, and mDNS advertisements to build an initial list of devices.
- The Probe connects to each device using supported protocols and gathers additional data such as CDP and LLDP adjacency tables, MAC address tables, and associated device lists.

- This information helps identify more devices, and the process repeats until all devices are discovered.

Q. Does Cisco Business Dashboard do network scans?

A. The Cisco Business Dashboard Probe does not actively scan the broader network. The Probe will use the ARP protocol to scan the IP subnet it is directly attached to, but will not attempt to scan any other address ranges. The Probe will also test each discovered device for the presence of a webserver and SNMP server on the standard ports.

For direct managed networks, you may optionally create a schedule profile to actively scan designated IP ranges for manageable devices. If this is done, then the dashboard will attempt to connect to webserver ports on each IP address in the specified ranges to determine if a device is manageable.

Q. How quickly does Cisco Business Dashboard detect when a device goes offline?

A. The detection time depends on the network management type:

- For Direct Managed networks, Dashboard typically generates an offline alert up to 20 minutes after a device without CBD connection goes down. If the CBD connection itself goes down, the device is marked offline immediately.
- For Probe Managed Networks, the detection time varies based on the protocol and monitoring interval. Detection time ranges from 1 minute to 16 minutes for a Software Probe. Detection time ranges from 12 minutes to 30 minutes for an Embedded Probe.

Actual detection time may vary depending on network conditions and configuration.

Q. Can I move a device from one network to another in Cisco Business Dashboard?

A. No, Cisco Business Dashboard does not support directly moving a device from one network to another. If devices are physically part of the same network - meaning they are connected or belong to the same VLAN - they will automatically discover each other using CDP, LLDP, or Bonjour, and the Dashboard will put them together in the same network. However, you can create separate device groups to apply specific configurations or monitoring profiles to each group as needed.

Q. How do I delete a device?

A. Only offline devices can be removed from the inventory. To delete an offline device, navigate to the **Inventory** page, select the desired device, and click the **Delete** icon located at the top of the table. Please note that online devices cannot be deleted; however, if you wish to exclude specific devices from your inventory list, you can configure a discovery filter by navigating to the **Discovery** tab within the network details page.

Configuration FAQs

Q. What happens when a new device is discovered? Will its configuration be changed?

A. New devices will be added to the default device group. If configuration profiles have been assigned to the default device group, then that configuration will be applied to newly discovered devices.

Q. What happens when I move a device from one device group to another?

A. Any VLAN or WLAN configuration associated with profiles that are currently applied to the original device group that are not also applied to the new device group will not change, and VLAN or WLAN configuration associated with profiles that are applied to the new group that are not applied to the original

group will be added to the device. System configuration settings will be overwritten by profiles applied to the new group. If no system configuration profiles are defined for the new group, then the system configuration for the device will not change.

Q. What should we do if a device shows a "Pending Configuration Out of Sync" or "Configuration Mismatch" status in Cisco Business Dashboard?

A. If a device displays a "Pending Configuration Out of Sync" or "Configuration Mismatch" status in Cisco Business Dashboard, you should:

1. Go to the Inventory page in Cisco Business Dashboard.
2. Select the affected device by clicking on its hostname to open its details page.
3. Check the "Pending Config" tab in the device details page.
4. If the current configuration in CBD is incorrect or outdated, click "Read Current Configuration" to retrieve the latest configuration from the device.
5. If the pending configuration is still out of sync after this, you can either:
   - Click "Accept Current Configuration" to replace the pending configuration with the current configuration from the device, or
   - Click "Apply Pending Configuration" to re-apply the pending configuration to the device.

Additionally, ensure that the device credentials are correct. If there are credential issues, update them in Administration > Device Credentials in the dashboard as needed.

Security Consideration FAQs

Q. What port ranges and protocols are required by Cisco Business Dashboard?

A. The following table lists the protocols and ports used by Cisco Business Dashboard:

Table 1: Cisco Business Dashboard - Protocols and Ports

Port	Direction	Protocol	Usage
TCP 22	Inbound	SSH	Command-line access to the Dashboard. SSH is disabled by default on the Cisco virtual machine image.
TCP 80	Inbound	HTTP	Web access to the Dashboard. Redirects to secure web server (port 443).
TCP 443	Inbound	HTTPS Multiplexed TCP	Secure web access to the Dashboard Communication between Probe and Dashboard.
UDP 1812	Inbound	RADIUS	Device access to the Dashboard when authenticating user access.

Port	Direction	Protocol	Usage
TCP 50000 - 51000 (Systems deployed from the Microsoft Azure marketplace use TCP 50000 - 50049)	Inbound	HTTPS	Remote access to devices. This range may be controlled using the System > Platform Settings page.
UDP 53	Outbound	DNS	Domain name resolution.
UDP 123	Outbound	NTP	Time synchronization.
TCP 443	Outbound	HTTPS	Access Cisco web services for information such as software updates, support status, and end of life notices. Access OS and application update services.
UDP 5353	Outbound	mDNS	Multicast DNS service advertisements to the local network advertising the Dashboard.
TCP 22	Outbound	SSH	CLI access to the device
UDP 53	Outbound	DNS	Domain name resolution

Q. What port ranges and protocols are required by Cisco Business Dashboard Probe?

A. The following table lists the protocols and ports used by Cisco Business Dashboard Probe:

Table 2: Cisco Business Dashboard - Protocols and Ports

Port	Direction	Protocol	Usage
TCP 22	Inbound	SSH	Command-line access to the Probe. SSH is disabled by default on the Cisco virtual machine image.
TCP 80	Inbound	HTTP	Web access to the Probe. Redirects to secure web server (port 443).
TCP 443	Inbound	HTTPS	Secure web access to the Probe.
UDP 5353	Inbound	mDNS	Multicast DNS service advertisements from the local network. Used for device discovery.
TCP 22	Outbound	SSH	CLI access to the device.
UDP 53	Outbound	DNS	Domain name resolution.
UDP 123	Outbound	NTP	Time synchronization

Port	Direction	Protocol	Usage
TCP 80	Outbound	HTTP	Management of devices without secure web services enabled.
UDP 161	Outbound	SNMP	Management of network devices.
TCP 443	Outbound	HTTPS Multiplexed TCP	Management of devices with secure web services enabled. Access Cisco web services for information such as software updates, support status, and end of life notices. Access OS and application update services. Communication between Probe and Dashboard.
UDP 5353	Outbound	mDNS	Multicast DNS service advertisements to the local network advertising the Probe.

Q. What Cisco servers does Cisco Business Dashboard communicate with and why?

A. The following table lists the Cisco servers that Cisco Business Dashboard communicates with, and the purpose of that conversation:

Table 3: Cisco Business Dashboard - Cisco Servers

Hostname	Purpose
*.firebaseio.com	Used to collect product improvement data and to support the Push notifications to Cisco Business Mobile App feature. This server is only used if product improvement is enabled in **System > Privacy Settings**, or if you use the Push notifications to Cisco Business Mobile App functionality.
api.cisco.com apix.cisco.com	Used to retrieve software update information and product lifecycle information. This server is only used if software updates or lifecycle reporting are enabled in System > Privacy Settings.
dl.cisco.com download-ssc.cisco.com softwarecloud.cisco.com	Used to download software update files from Cisco. These servers are only used if software updates are enabled in **System > Privacy Settings** and you execute an upgrade operation for a network device or for Cisco Business Dashboard.
smb-ai.cbd-aws.com	Used by AI Assistant.
cloudsso.cisco.com id.cisco.com	Used to authenticate Cisco Business Dashboard prior to communicating with api.cisco.com. This server is only used if software updates or lifecycle reporting are enabled in **System > Privacy Settings**.

Hostname	Purpose
www.cisco.com	Used to retrieve updates to the root certificate authority signing certificates used to verify X509 certificates used by Cisco and third-party services to secure network communication.

Q. What processes and system services are required by Cisco Business Dashboard?

A. The following table lists the processes and system services used by Cisco servers that Cisco Business Dashboard:

Table 4: Cisco Business Dashboard - Processes and System Services

Process	Additional Details
Dashboard Essential Processes	
/usr/lib/jvm/java-x-openjdk-amd64/bin/java … -jar /usr/lib/ciscobusiness/dashboard/lib/nm-aio-application-x.x.x-SNAPSHOT.jar	The main dashboard application
/usr/lib/ciscobusiness/dashboard/bin/nginxsvc /usr/lib/ciscobusiness/dashboard/bin/nginx	Web Server
/usr/lib/ciscobusiness/dashboard/bin/mongosvc /usr/lib/ciscobusiness/dashboard/bin/mongod /usr/lib/postgresql/xx/bin/postgres postgres: xx/main:	Database services
/bin/bash /usr/lib/ciscobusiness/dashboard/bin/freeradiussvc /usr/lib/ciscobusiness/dashboard/bin/freeradius	User authentication services
/usr/lib/ciscobusiness/dashboard/bin/redissvc /usr/lib/ciscobusiness/dashboard/bin/redis-server	In-memory cache services
/usr/lib/ciscobusiness/dashboard/bin/rabbitmqsvc /usr/lib/ciscobusiness/dashboard/bin/rabbitmq-server /usr/lib/erlang/erts-xx.x.x.xx/bin/epmd /usr/lib/erlang/erts-xx.x.x.xx/bin/epmd.smp erl_child_setup	Message broker
/usr/lib/ciscobusiness/dashboard/bin/bonjoursvc avahi-publish	Multicast DNS announcements
Dashboard Essential System Services	
/usr/sbin/rsyslog	Logging services
/usr/sbin/cron	Scheduling services
systemd-timesyncd	Time services

Process	Additional Details
Dashboard Essential Processes	
avahi-daemon	Multicast DNS listener

Q. What processes and system services are required by Cisco Business Dashboard Probe?

A. The following table lists the processes and system services used by Cisco servers that Cisco Business Dashboard Probe:

Table 5: Cisco Business Dashboard - Processes and System Services

Process	Additional Details
Probe Essential Processes	
/usr/lib/ciscobusiness/probe/bin/cbdprobe chagent	The main probe application
/usr/lib/ciscobusiness/probe/bin/fpscan	Device scanning tool
/usr/lib/ciscobusiness/probe/bin/main /usr/lib/ciscobusiness/probe/bin/publish avahi-publish	Multicast DNS announcements
nginx	Web server When collocated on a dashboard server, the probe shares the dashboard web server
Probe Essential System Services	
/usr/sbin/rsyslogd	Logging services
/usr/sbin/cron	Scheduling services
systemd-timesyncd	Time services
avahi-daemon	Multicast DNS listener
lldpd	LLDP neighbor discovery

Q. How secure is the communication between Cisco Business Dashboard and a device/Probe?

A. All communication between the Dashboard and the device/Probe is encrypted using a TLS 1.2 session authenticated with server certificates. The session is initiated from the device/Probe to the Dashboard.

Q. Does Cisco Business Dashboard have ‘backdoor’ access to my devices?

A. No. When Cisco Business Dashboard discovers a supported device, it will attempt to access the device using the factory default credentials for that device with the username and password: `cisco`, or the

SNMP community:`public`. If the device configuration has been changed from the default, then it will be necessary for the user to supply correct credentials to Cisco Business Dashboard.

Q. How secure are the credentials stored in Cisco Business Dashboard?

A. Credentials for accessing Cisco Business Dashboard are irreversibly hashed using the SHA512 algorithm. Credentials for devices and other services, such as the **Cisco Active Advisor**, are reversibly encrypted using the AES-128 algorithm.

Q. How do I recover a lost password for the web UI?

A. If you have lost the password for all the admin accounts in the web UI, you can recover the password by logging on the console of the Probe and running the **cbdprobe recoverpassword** tool, or logging on the console of the Dashboard and running the **cisco-business-dashboard recoverpassword** tool. This tool resets the password for the cisco account to the default of cisco, or, if the cisco account has been removed, it will recreate the account with the default password. Following is an example of the commands to be provided in order to recover the password using this tool.

```
cisco@cisco-business-dashboard:~$ cisco-business-dashboard recoverpassword
Are you sure? (y/n) y
Recovered the cisco account to default password
recoverpassword Cisco Business Dashboard successful!
cisco@cisco-buisness-dashboard:~$
```



Note When using Cisco Business Dashboard for AWS, the password will be set to the AWS instance ID.

Q. What is the default username and password for the Virtual Machine bootloader?

A. The default credentials for the Virtual Machine bootloader are username: **root** and password: **cisco**. These may be changed by running the config_vm tool and answering yes when asked if you want to change the bootloader password.

Q. How does the dashboard authenticate network access devices?

A. The dashboard uses two levels of authentication.

- First, the source IP address of the incoming request is compared with the external IP address(es) of the networks managed by the dashboard when NAT is in use, or the internal subnets of the networks when there is no NAT in use.
- Second, a unique, randomized RADIUS secret is created for each organization and must be used by the network access device in its request.

Q. Will the AI Assistant share your personal data with Cisco?

A. The AI Assistant operates based of a large language model (LLM) which is designed to provide responses to your queries based on the questions it receives. It does this without collecting or storing any of your

personal (PII) data. It does, however, retain past conversations you have had so you can easily reference them in the future.

Q. Is my data being used to train the AI Assistant?
A. No, your data is not used to train the AI Assistant.

Remote Access FAQs

Q. When I connect to a device's administration interface from Cisco Business Dashboard, is the session secure?
A. Cisco Business Dashboard tunnels the remote access session between the device and the user. The protocol used between the Probe and the device will depend on the end device configuration, but Cisco Business Dashboard will always establish the session using a secure protocol if one is enabled (e.g. HTTPS will be preferred over HTTP). If the user is connecting to the device via the Dashboard, the session will pass through an encrypted tunnel as it passes between the Dashboard and the Probe, regardless of the protocols enabled on the device. The connection between the user's web browser and the Dashboard will always be HTTPS.

Q. Why does my remote access session with a device immediately log out when I open a remote access session to another device?
A. When you access a device via Cisco Business Dashboard, the browser sees each connection as being with the same web server (the Dashboard) and so will present cookies from each device to every other device. If multiple devices use the same cookie name, then there is the potential for one device's cookie to be overwritten by another device. This is most often seen with session cookies, and the result is that the cookie is only valid for the most recently visited device. All other devices that use the same cookie name will see the cookie as being invalid and will logout the session.

Q. Why does my remote access session fail with an error like the following? **Access Error: Request Entity Too Large HTTP Header Field exceeds Supported Size**
A. After doing many remote access sessions with different devices, the browser will have a large number of cookies stored for the Dashboard domain. To work around this problem, use the browser controls to clear cookies for the domain and then reload the page.
Q. When I connect to a device's command line interface from Cisco Business Dashboard, is the connection secure?
A. Yes, the connection is secure. Cisco Business Dashboard tunnels the remote CLI console access session between the device and the user through an encrypted tunnel. The protocol used to access device is SSH. The connection between the user's web browser and the Dashboard will always be HTTPS.

Software Update FAQs

Q. How do I keep the Dashboard operating system up to date?
A. The Dashboard uses the Ubuntu Linux distribution for an operating system. The packages and kernel may be updated using the standard Ubuntu processes. For example, to perform a manual update, log on to the console as the cisco user and enter the commands `sudo apt-get update` and `sudo apt-get upgrade`. The system should not be upgraded to a new Ubuntu release, and it is recommended that no

additional packages should be installed beyond those included in the virtual machine image supplied by Cisco, or those installed as part of a minimal Ubuntu install.

Q. How do I update Java on the Dashboard?

A. Cisco Business Dashboard uses the OpenJDK packages from the Ubuntu repositories. OpenJDK will automatically be updated as part of the updating the core operating system.

Q. How do I keep the Probe operating system up to date?

A. Cisco Business Dashboard uses the Ubuntu Linux distribution for an operating system. The packages and kernel may be updated using the standard Ubuntu processes. For example, to perform a manual update, log on to the console as the cisco user and enter the commands `sudo apt-get update` and `sudo apt-get upgrade`. The system should not be upgraded to a new Ubuntu release, and it is recommended that no additional packages should be installed beyond those included in the virtual machine image supplied by Cisco, or those installed as part of a minimal Ubuntu install.

Q. How do I keep the Probe operating system up to date when using a Raspberry Pi?

A. The Raspbian packages and kernel may be updated using the standard processes used for Debian-based Linux distributions. For example, to perform a manual update, log on to the console as the cisco user and enter the commands `sudo apt-get update` and `sudo apt-get upgrade`. The system should not be upgraded to a new Raspbian major release. It is recommended that no additional packages are installed beyond those installed as part of the 'Lite' version of the Raspbian distribution and those that are added by the Probe installer.

Q. I see that Cisco Business Dashboard 2.7.0 adds support for Ubuntu 22.04 (Jammy Jellyfish). If I have upgraded my system to 2.7.0, can I upgrade the operating system from Ubuntu 20.04 to Ubuntu 22.04?

A. Unfortunately, the changes between the two operating system releases are too great to allow an in-place upgrade. If your current system is running Ubuntu 20.04, you should upgrade the dashboard to release 2.7.0 and then follow these steps to successfully upgrade to a Dashboard based on Ubuntu 22.04:

1. Take a backup from the existing Cisco Business Dashboard instance.
2. Please ensure to release any device licenses currently allocated to the existing Dashboard instance. To accomplish this, navigate to the System > License page, and select Deregister… from the drop-down list located at the top right.
3. Shutdown the current Dashboard server. The restoration process may assign the new server the same IP address as the current server, leading to a potential IP conflict. To prevent this, it is critical to shut down the current server prior to restoration.
4. Install a fresh Dashboard instance with latest version, then restore the backup file taken in step 1 to this new instance.
5. Please ensure the Dashboard server address remains consistent after restoration to allow connected devices to reconnect seamlessly. If using a domain name, update the DNS to point to the new Dashboard instance. For AWS or Azure, assign the same public IP address to the new Dashboard instance.